Homework 5

CMSY-199, Fall 2013

Upload your solution to the Canvas course website as a zip archive file prior to the start of class on Monday, November 18.

An Enigma machine is an electro-mechanical rotor cipher machine used for enciphering and deciphering secret messages. It consists of a keyboard, mechanical rotors, and a lampboard through which an electrical current flows. The Enigma I is a specialized version used by the German military during World War II in which a plugboard was added to increase the cryptographic strength. It also has a fixed reflector and rings to adjust the path of the electrical current relative to the wiring of the rotors.

The keyboard consists of the 26 letters of the English alphabet, and each key press causes one or more of the three rotors to step by one twenty-sixth of a full rotation (before the electical connection is made) producing a polyalphabetic substituion cipher. The right rotor steps once each key press, while the center and left rotors step less frequently. Each rotor has a single notch that causes its neighbor to the left to advance one position. A consequence of the actual design causes double-stepping of the center rotor on the same key press when a step of the right rotor causes the center rotor to step into its notch position.

The reflector reversed the direction electrical current passing it back through the rotors along a different path to the lampboard where the output letter would be illuminated. Since the reflector was fixed and connected the output of the left rotor into pairs, it ensured that encryption and decryption were reciprocal. That is, an encrypted message could be decrypted by setting the machine to the same initial state, typing the encrypted message into the keyboard, and observing the decrypted message output on the lampboard.

The plugboard allowed for as many as 13 pairs of letters to be connected with cables switching the connections of those letters between the keyboard and the rotors. In addition to the selection and order in which the rotors were inserted into the machine, each rotor had a ring setting which allowed for and additional offset of the letters relative to the rotor wiring.

In all, the Enigma I machine's initial state consisted of the choice of rotors and the order in which they were inserted, the initial position of each rotor, the ring settings for each rotor, and the plugboard connections.

1. Design and implement a simplified Enigma I machine in Java using the object-oriented programming concepts that were presented in class. In order to simplify the assignment, you may assume that no plugboard connections have been made and the ring settings of each rotor have not been adjusted from their default positions. Additionally, you will have one of each of the three rotors (always inserted with rotor I on the left, rotor II in the center, and rotor III on the right) and the single reflector described below.

Rotor	Notch	Wiring
I	Q	E K M F L G D Q V Z N T O W Y H X U S P A I B R C J
II	E	A J D K S I R U X B L H W T M C Q G Z N P Y F V O E
III	V	B D F H J L C P R T X V Z N Y E I W G A K M U S Q O

Reflector	Wiring
B	Y R U H Q S L D P X N G O K M I E B F Z C W V J A T

2. The example on the next page illustrates that when the letter C is pressed on the keyboard with rotors I, II, and III set to the initial positions M, L, and M, respectively, the letter V is illuminated on the lampboard. The letters with the thick border on the left side are displayed in the indicator panel of each rotor. Electrical connections are shown in yellow moving inward from the keyboard and red moving outward toward the lampboard. Each connection is numbered and indicates the order in which it was made.

3. There are a number of excellent references on the internet regarding enigma machines.

   (a) http://en.wikipedia.org/wiki/Enigma_machine

   (b) http://en.wikipedia.org/wiki/Enigma_rotor_details

   (c) Solving the Enigma: History of the Cryptanalytic Bombe

   (d) How Mathematicians Helped Win WWII

   (e) http://www.bletchleypark.org.uk/

   (f) Paper Enigma Machine

4. Enigma machine simulator implementations are available from the internet, the Apple App store, and Google Play. It is okay to use these to verify your own implementation, but *do not* browse their source code. Your design and implementation must be your own work.

Keyboard / Lampboard	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rotor III	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O	B	D	F	H	J	L	C	P	R	T	X	V
	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
Rotor II	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E	A	J	D	K	S	I	R	U	X	B	L
	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
Rotor I	O	W	Y	H	X	U	S	P	A	I	B	R	C	J	E	K	M	F	L	G	D	Q	V	Z	N	T
	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
Reflector B	Y	R	U	H	Q	S	L	D	P	X	N	G	O	K	M	I	E	B	F	Z	C	W	V	J	A	T
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Keyboard / Lampboard	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
			1																			8				
Rotor III	N	Y	E	I	W	G	A	K	M	U	S	Q	O	B	D	F	H	J	L	C	P	R	T	X	V	Z
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
					7													2								
Rotor II	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E	A	J	D	K	S	I	R	U	X	B	L
	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
																		6	3							
Rotor I	O	W	Y	H	X	U	S	P	A	I	B	R	C	J	E	K	M	F	L	G	D	Q	V	Z	N	T
	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
																				5						4
Reflector B	Y	R	U	H	Q	S	L	D	P	X	N	G	O	K	M	I	E	B	F	Z	C	W	V	J	A	T
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z